the smoking gun SINCE 1997 SEARCH

HOME • DOCUMENTS • BUSTER • BACKSTAGE • MUG SHOTS • TIME WASTER ABOUT •

DOCUMENT: Internet, Crime

JANUARY 6, 2014

"Guccifer" Files Further Detail Hacking Spree

Online outlaw's "archive" reveals scores of new victims

Tweet 408 You and 1,481 others like this.1,481 people like this. Sign Comments(98) Share

1/22 UPDATE: *"Guccifer" has been arrested, according to Romanian officials*

JANUARY 6--The hacking spree by "Guccifer," the online outlaw who has bedeviled Colin Powell, members of the Bush and Rockefeller families, Obama administration officials, and assorted other public figures, has been far more extensive than previously known, The Smoking Gun has learned.

A large cache of documents reveals that the illegal "Guccifer" incursions have victimized scores of other high-profile victims both in the U.S. and overseas during the past year. The hacker has accessed e-mail correspondence, contact lists, phone records, personal photos, online storage sites, and a wide range of confidential financial documents, including credit card, banking, and investment statements.

SUBMIT A TIP!

The newest roster of "Guccifer" victims includes entertainers, industrialists, academics, diplomats, financiers, government and military officials, and journalists--most of whom likely have no idea that the hacker has illegally prowled through their online accounts. With few discernible patterns, "Guccifer" has hopscotched between the accounts of victims like comedian Steve Martin; editor Tina Brown (seen below); ex-Nixon aide John Dean; author Kitty Kelley; actress Mariel Hemingway; three members of the UK's House of Lords; a former Air Force secretary; the CEO/chairman of MetLife, the $60 billion insurance conglomerate; a Pulitzer Prize winner; the director of Romania's domestic intelligence service; and a Gibson Dunn partner with the improbably Dickensian name Cantwell F. Muckenfuss III.

Along the way, "Guccifer" has also gathered the cell phone numbers of Robert Redford and Warren Beatty, the private e-mail addresses for Nicole Kidman, Leonardo DiCaprio, and other celebrities, and even the script for the fourth-season finale of "Downton Abbey" (which the hacker swiped six months before the TV episode first aired in England).

The material detailing Guccifer's felonious escapades was provided to TSG by the hacker himself, whose identity, location, and gender remains unknown (though for narrative purposes we'll refer to the hacker as a "he").

"i don't know what near future hold for me," the hacker stated, adding that the thousands of documents were being provided to a reporter "in case I disappear." Aware that a platoon of federal agents is hunting for him (or her or them), "Guccifer" facetiously claimed to be having dreams "in which a woman is steping up to me saying that she is

The Smoking Gun

You like this.

You and 72,928 others like The Smoking Gun.72,928 people like The Smoking Gun.

FEATURED

DOCUMENT: Crime NOVEMBER 26, 2014

Woman Arrested For $6400 Sausage Heist

Cops: Perp, 45, swiped pallet of products from Texas employer

DOCUMENT: Crime NOVEMBER 24, 2014

Police Continue Probing Brown Family Brawl

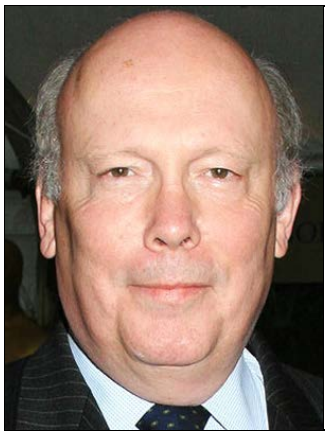
DOCUMENT: K-12, Crime NOVEMBER 24, 2014

Cops: Teacher Sought Student Silence Over Sex

from Federal Bureau and I am busted." He added, "meanwhile me trying desperately to erase my files on my computer at my desk or on my smartphone which btw I don"t have because I can"t afford one."

Included in the archive are documents amounting to the hacker's work product, such as text files recording an individual victim's name, e-mail address, original account password, and the replacement password used by "Guccifer." For instance, when the hacker broke into Powell's e-mail account, the password was changed to "ASSHOLEANON." After breaching the Comcast e-mail account of John Negroponte, a former U.S. ambassador to the United Nations, "Guccifer" reset the password to "hondbabykill1," an apparent reference to Negroponte's prior role as U.S. ambassador to Honduras, where American officials supported a military dictatorship suspected of killing and torturing dissidents.

While "Guccifer" has declined to discuss how he has been able to hack so many e-mail accounts--spanning an array of providers like Comcast, Cox, Gmail, Yahoo, AOL, Earthlink, Verizon, and the British-based Btinternet--it appears he compromised some accounts by correctly guessing security questions. Work files show that the hacker reviewed the Wikipedia pages of prospective victims, obtained the names of a target's relatives, and even referred to a list containing the most popular names for dogs and cats.



Last spring, "Guccifer" hacked a Yahoo account maintained by an assistant to Brown, then editor of The Daily Beast web site. Along with reading correspondence and stealing family photos, the hacker copied Brown's address book, which contained nearly 900 names and corresponding e-mail addresses. He then exported Brown's contacts into an Excel spreadsheet and began reviewing the lengthy list for possible new targets, a standard "Guccifer" M.O..

While the hacker routinely copies an address book following a break-in, some contact lists--like those of Brown, Powell, and former White House adviser Sidney Blumenthal--have proven to be target-rich environments for "Guccifer" to exploit.

For example, armed with Brown's contact list, "Guccifer" highlighted dozens of names--most with either AOL or Earthlink accounts--for illegal scrutiny. The hacker's spreadsheet memorialized his hacking of the e-mail accounts of journalist Carl Bernstein, "Sex and the City" author Candace Bushnell, actor Rupert Everett, BBC broadcaster Jeremy Paxman, and others. The color-coded Excel file also shows that "Guccifer" eyed the e-mail accounts of Lorne Michaels, Candice Bergen, Eric Idle, Whoopi Goldberg, Padma Lakshmi, Mike Nichols, and Isaac Mizrahi (though it is unclear if these accounts were breached). The hacker's archive also reveals that he was researching Martin Amis in preparation for an assault on the author's Yahoo account.

"Guccifer" used Brown's account to obtain the e-mail address of Julian Fellowes (seen above), the British actor/writer who created "Downton Abbey," and is also a member of the House of Lords. Somehow, the hacker subsequently broke into Fellowes's Btinternet account and copied a variety of correspondence as well as confidential records related to the 64-year-old's writing and political careers. One of the documents stolen last May by "Guccifer" was Fellowes's script for the finale of the latest season of "Downton Abbey." The hacker, however, apparently did not seek to disseminate the script for the last episode (which aired in England two months ago).

Fellowes is not the only House of Lords member to be victimized by "Guccifer." Documents show that the hacker also raided the e-mail accounts of Sir Francis Brooke and Patricia Scotland, who served previously as the UK's Attorney General. Scotland's SkyDrive online storage account was also breached.

In an interview, Brown said that she had been

MOST POPULAR

1. BUSTER: Michael Brown's Stepfather Urged Protesters To "Burn This Bitch Down" After Grand Jury Announcement

2. BUSTER: Ferguson Witnesss Told Investigators That Michael Brown Charged Cop "Like a Football Player. Head Down"

3. DOCUMENT: Police Continue Probing Brown Family Brawl

4. DOCUMENT: Cops: Teacher Sought Student Silence Over Sex

5. DOCUMENT: Woman Arrested For $6400 Sausage Heist

Tucson, AZ Residents Are 'Rattled' By New Website

unaware that her account had been breached by "Guccifer," adding that it was upsetting to learn that some of her contacts had been hacked as a result. A Brown assistant, who recalled getting notices that the Yahoo account's password had been changed, forwarded an e-mail that was sent from the account in May to a second Brown aide. The subject line read "i will fuck u an you wiil never know." The aide told TSG, "Nice email from Mr. Guccifer, huh?"

The "Guccifer" archive includes documents memorializing the hacking of the e-mail accounts of dozens of other individuals. These victims include:

***** Hemingway, whose AOL account was broken into early last year. That incursion yielded passwords to the 52-year-old star's web site and Facebook page (which "Guccifer" defaced in late-February). In a note to her followers, a disgusted Hemingway (pictured above) reported being hacked, noting that she "changed everything UGH makes you feel violated."

***** Steven Kandarian, the MetLife chief executive, had his Comcast account raided by "Guccifer," who stole the 60-year-old businessman's contact list, divorce records, phone logs, and a variety of personal financial records.

***** George-Cristian Maior, head of the Romanian Intelligence Service, had his Yahoo account breached.

***** George Roche, a former Secretary of the Air Force, was one of more than a dozen former U.S. military officials who had their accounts illegally accessed by "Guccifer." Most of these victims, Roche included, had e-mail accounts with Comcast, a company the hacker seems to have little trouble compromising.

***** Kelley had her Yahoo and Earthlink accounts compromised early last year. "Guccifer," who apparently found the biographer's e-mail address in Blumenthal's contact list, read through her e-mails and took months worth of Kelley's cell phone bills, which listed numbers she dialed as well as calls she received. Kelley told TSG she was unaware of the hacking, but recalled that "Earthlink changed my password twice, I think, without explanation."

***** Laura Manning Johnson, a top Department of Homeland Security official and former CIA analyst. "Guccifer" breached her Comcast account in mid-2013.

***** Pulitzer Prize-winning author Diane McWhorter, whose Earthlink, Gmail, and Dropbox storage accounts were raided. "Guccifer" apparently found McWhorter's e-mail among Blumenthal's contacts.

***** Dean's Earthlink account was hacked early last year, and "Guccifer" took family photos, assorted correspondence, and personal financial records.

***** Fitness instructor Denise Austin was hacked early last year. Her Comcast account was broken into shortly after "Guccifer" illegally accessed the e-mail account of Dorothy Bush Koch, sister of George W. Bush (and daughter of George H.W. Bush). Austin's e-mail address was in Koch's contact list, which the hacker copied.

***** Oceanographer Robert Ballard, who was part of the team that located the Titanic's wreck, had his Comcast e-mail and Dropbox accounts hacked by "Guccifer." Ballard, seen below, was apparently targeted because his name

appears on a roster of members of Bohemian Grove's Mandalay Camp. The hacker found the list in the AOL account of Powell, who is also a Mandalay member (along with Henry Kissinger and George Shultz, both of whom are also former Secretaries of State. In e-mails last year, "Guccifer" asserted that attendees at Bohemian Grove's northern California retreats were part of the shadowy Illuminati/New World Order conspiracy "leading this fucked up world!!!!!"

***** Muckenfuss, a Washington, D.C. attorney and Yale Law School lecturer, had two of his e-mail accounts breached by "Guccifer." It appears the hacker found the 68-year-old lawyer's Comcast e-mail address in the Gmail contact list of Joshua Gotbaum, director of the Pension Benefit Guaranty Corporation. After hacking Gotbaum's account last May, "Guccifer" took the Obama appointee's address book and used it to victimize several of Gotbaum's acquaintances.

The "Guccifer" archive shows that he also accessed the e-mail accounts of numerous members of the Council on Foreign Relations. The hacker obtained the e-mail addresses of hundreds of CFR figures after he broke into the account of one member and accessed private contact lists.

Additionally, the hacker's work product reveals that he illegally accessed the e-mail of a New York company that handles security matters for corporations and wealthy individuals. "Guccifer" took a variety of reports detailing confidential work done by the firm, including a $40,000 security review commissioned by a hedge fund billionaire who wanted assurances that a duplex apartment his daughter, a college student, planned to rent while studying in Paris was safe.

While "Guccifer" has repeatedly declined to discuss how he breaks into accounts--he has dismissed these TSG queries as "irrelevant extraneous technical questions"--some targets have eased his path through their online lives.

For example, two victims--a writer and an ex-FBI agent--each kept Word files containing numerous password and PIN numbers they used. Combined, the two documents (which were found in the "Guccifer" archive) offered free access to accounts with eBay, Netflix, PayPal, Xbox, Amazon, Sprint, Etsy, Facebook, Dropbox, Time Warner, and Skype. Not to mention credit card, banking, insurance, retirement, and frequent flyer accounts. The former G-man's list even included a three-digit password for a "Gun Lock."

The illegal incursions into these two accounts emanated from IP addresses in Greece and the Russian Federation, according to the victims.

Other records show that "Guccifer" has sought to monitor, albeit to a limited degree, the federal criminal probe targeting him.

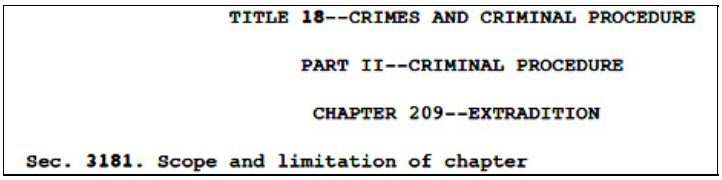
For instance, after TSG reported the hacking of several Bush family e-mail accounts--most notably the AOL account of Dorothy Bush Koch--"Guccifer" lost control over those accounts. He still, however, was able to monitor the hacked account of Koch's friend Patricia Legere. Which allowed him to read an e-mail from Koch informing friends and family that her account had been compromised and that Secret Service agents were en route to her residence to collect her computer for analysis.

Similarly, after "Guccifer" hacked the e-mail and Facebook accounts of an Obama administration appointee, he somehow maintained access to the victim's telephone records. Those documents, "Guccifer" discovered, revealed that the FBI contacted the federal official immediately after the hacking was reported by TSG.

Though publicizing his continuing criminal activity could provide federal agents with new leads and investigative avenues to pursue, "Guccifer" professed to be carefree despite his status as one of America's most wanted hackers: "NO I am not concerned, i think i switch the proxies go to play some backgammon on yahoo watch tv, play with my family and daughter." The hacker wrote of buying

a “new powerful computer” to help continue his illegal activities. Noting that he would be “back in business,” “Guccifer” closed one e-mail with a one-word declaration: “HAAAACKKKK!”

In other correspondence, “Guccifer” has written of living overseas, though that could be a feint from a hacker who has spent more than a year using proxy servers, fake IP addresses, burner e-mail accounts, anonymizing software, and other methods to evade pursuing law enforcement authorities.



TITLE 18--CRIMES AND CRIMINAL PROCEDURE

PART II--CRIMINAL PROCEDURE

CHAPTER 209--EXTRADITION

Sec. 3181. Scope and limitation of chapter

“Guccifer” wrote of turning over his archive “just in case I am busted,” but he has not offered a rationale for the crime spree detailed in those documents. While referring to his distaste for the “new ukusa empire,” the hacker claims to be operating from “the cloud of Infinite Justice.” Still, it is hard not to view many of his break-ins as crimes of opportunity. Hacking for hacking’s sake, with a simple goal of disruption, havoc, and embarrassment.

Which, of course, does not make his frenzied rampage any less felonious. In fact, two files in the “Guccifer” archive appear to show the hacker researching possible criminal charges in a United States court. A 76-page Congressional Research Service report explores the “Extraterritorial Application of American Criminal Law,” while the other file includes the section of the U.S. Code detailing the country’s extradition law and treaties.

Perhaps these documents indicate that “Guccifer” thinks the end is near. Or maybe he just stole them from somebody’s Inbox.

Tweet 1.4k

TAGS:
Guccifer, Hacking, Bush Hack, Colin Powell, Tina Brown, Kitty Kelley, Julian Fellowes

PREV DOCUMENT
Novelist's Ex In Bizarre Handgun Threat Arrest

DOCUMENT NEXT
Here's One Guy Who Will Never Forget The Alamo

We Recommend

Sponsored Links by Taboola

Selfies Gone Wrong: 17 Most Embarrassing Celeb
Answers.com

Jennifer Lawrence's Beverly Hills Home Is Beyond Extravagant
LonnyMag

Looking for New Boots? Check out these AMAZING
Zulily

10 Celebs You'd Never Guess Went Full Frontal On Film
Suggest

4 Things You Should Never Buy at Trader Joe's
Reviewed.com

26 Things You Probably Didn’t Know About the Original
Vulture

You need to accept third-party cookies in your browser in order to comment using this social plugin.

98 comments Add a comment

Add a comment...

Also post on Facebook

Vic Shubin · Top Commenter
I wonder if Gucifer is really the NSA?
Reply · Like · 84 · January 6 at 5:50pm

Ziegler Von Strahn · Top Commenter
if not already....he will be when they catch him.
Reply · Like · 14 · January 6 at 7:06pm

Vic Shubin · Top Commenter
Maximilian Vila FMC? I used to work in FMC's AI labs (CTC) in San Jose. Wow!
Reply · Like · 1 · January 6 at 7:45pm

Ron Demarais · Top Commenter
What difference is there?
Reply · Like · January 7 at 5:04am

View 5 more

Add a Reply...

Don Newman · Top Commenter
I hope Gucifer doesn't hack my email and get that 500k I won in the South African Lottery. I really do need to reply to that email eventually.
Reply · Like · 64 · January 6 at 10:51pm

Bryan Wilcutt · Top Commenter
I'm still waiting for my African uncle's estate trustee to send me my billion dollar inheritance. I had a rich black uncle. Who knew???
Reply · Like · 29 · January 7 at 7:59am

George Koehler · Top Commenter · St. Philip's College
Yeah, me too, my email says he's from Nigeria! I hope he looks me!!!
Reply · Like · 10 · January 7 at 11:10am

StefanStein Verleysen · Shippensburg University of Pennsylvania
ROFL
Reply · Like · 3 · January 16 at 5:16am

View 5 more

Add a Reply...

David Brown · Top Commenter · Chief Executive Officer at World Federation of Iconoclasts · 134 followers
Guccifer should realize that the gubernut don't like no competition.
Reply · Like · 44 · January 6 at 6:33pm

Bang Stick · Top Commenter
They'll just give him a job with a 6, maybe 7 figure salary and he can carry on with govt approval.
Reply · Like · 19 · January 6 at 7:36pm

Jeffrey Gee · Top Commenter · Virginia Western Community College

An Itsybit Kicking a dumb phone still over here. Sadly, I have an Electrical Engineering degree you'd figure I would keep up with the times...

Reply · Like · January 23 at 8:27am

Add a Reply...

Chris Clinkinbeard · Top Commenter · Park Hills, Kentucky

You know, as long as "Guccifer" remains non-partisan, I'm all for it. Bring all these assholes down.

Reply · Like · 38 · Edited · January 6 at 9:24pm

Chad Candland · Top Commenter · Salt Lake City, Utah

Seriously.

Reply · Like · 2 · January 8 at 2:16pm

Fig Nutts · Top Commenter · Parasite at Public Sector Leech

May be one of the few things lefties and righties can both agree on.

Reply · Like · 4 · January 22 at 9:04am

Add a Reply...

Monica Mazzuca · Top Commenter · Farmington, Connecticut

Please Gucifer.....Find Ovomits REAL birth cirt, and Phony SS number...And his College records, that probly says he was a forien exchange student ...EXPOSE HIM GUCIFER!!! PLEASE!!!

Reply · Like · 35 · January 7 at 8:34am

Will Smith · Top Commenter · University of North Florida (Official Fan Page)

Perhaps he can find Soros' personal data too. Get him Guccifer!

Reply · Like · 9 · January 22 at 11:55am

Jeffrey Gee · Top Commenter · Virginia Western Community College

All good ideas...Or who funded 9-11-2001. Though, it is already known in classified commission reports.

Reply · Like · 2 · January 23 at 8:31am

Add a Reply...

Kenneth E. Lamb · Top Commenter · Expert Witness in computer crimes at CyberSmart! Computers

Let me see if I understand this . . .

Guccifer and the NSA are doing exactly the same thing - illegally hacking into people's lives.

When Guccifer does it, the hackees are "outraged" and "shocked" - when the NSA does it, and digs up even more dirt than they can imagine, they yawn.

Guccifer merely embarrasses the hackees with the revelations. Can anyone honestly say exactly what the NSA does with its hacking information? Can you spell "Blackmail"?

Guccifer and the NSA are peas in a pod. Both are criminals, but only Guccifer will be prosecuted.

The NSA will commit perjury, admit to committing felonies on

thousands of people, and rely on a secret court making secret decisions that even a Supreme Court Justice can't read if the NSA deems the information "classified" beyond the Justice's "security clearance" - for which the Jus... See More

Reply · Like · 25 · Edited · January 7 at 8:38am

Add a Reply...

Monica Mazzuca · Top Commenter · Farmington, Connecticut

X-POSE HARRY REID AND NANCY PELOSI!!!!! Please, if your going to hack...x-pose the people ruining this country. Help us get RID of them once and for all.

Reply · Like · 18 · January 7 at 8:45am

Add a Reply...

Francisco Yruegas · American InterContinental University

If Grucifer really wanted to stop the "shadowy Illuminati/New World Order" he should put out a step by step tutorial on how he does what he does, shower the world with individual hackers. imagine the panic it would cause the those trying to keep all their actions uncover...

Reply · Like · 17 · January 7 at 7:35am

Add a Reply...

Patricia Holman · Top Commenter · Bakersfield, California

Gucifer you need to start checking on the crooked politicians. Check on Jerry Brown and see how much cash he's pocketing for pushing the high speed rail fiasco in California.

Reply · Like · 14 · January 6 at 10:12pm

Ra Williams · Top Commenter

Did he find a birth certificate from KENYA?

Reply · Like · 1 · January 23 at 9:44am

Add a Reply...

Roy Wagner · Top Commenter

Anybody here storing their Data in an "On Line" Storage provider? Still? Really?

Reply · Like · 10 · January 6 at 6:45pm

Chad Candland · Top Commenter · Salt Lake City, Utah

Hell they can Hot Mic any OS or phone. Cloud or at home its simple to get data. Hopefully one of our Senators here in Utah will grow some balls and sponsor a bill to cut the water and power to the data center they just built here.

Reply · Like · 4 · January 8 at 2:20pm

Add a Reply...

Dave Blackmoore · Top Commenter · Sonora, California

Is guccifer a code word for the NSA?

Reply · Like · 10 · January 6 at 7:16pm

Add a Reply...

Edward Riepe · Top Commenter · Time traveler at RER Publishing. at Self Employed Entrepreneur · 189 followers

Guccifer, I am the author or FEMA Camp 37, which the government hates. I am also not only the author but publisher Finding my email should be easy for you. Send me what you want to say and it will be on Amazon in twelve hours. We will work out the money later for your lawyers.

Reply · Like · 9 · January 6 at 8:59pm

Edward Riepe · Top Commenter · Time traveler at RER Publishing. at Self Employed Entrepreneur · 189 followers

Rory Macmillan No, that would be Guccifer's job. As a publisher I am offering him an opportunity to say what he wants to say.I am the author of FEMA Camp 37, FEMA Camp 43, Sin City Prison, Starvation Nation and the Red, the White and True Blue, all related fictional tales that entertain. I think Obama loves them. lol

Reply · Like · 1 · January 15 at 1:46am

Alex Ghita · Top Commenter · Colegiul National A.T.Laurian

Edward Riepe he just got arrested. he doesn't need to much money for lawyers and such, as, in our country, the punishment for hacking without financially benefiting from it is 2-5 years parole. if you make a profit from it, it's straight to jail 3-15y . and the judges don't really care about arguments like "well i made the money from telling the story of hacking, not the actual hacking". they'll say "you hacked, are you richer because of it, therefore you go to jail". we have a bit of common sense left in the judicial system.

Reply · Like · 1 · January 22 at 4:31pm

Add a Reply...

Cathy Lee · Top Commenter · Tampa, Florida

the smoking gun

© 2014 TSG Industries Inc.
All Rights Reserved.